

## CLAIMS

What is claimed is:

- 1    1. A method of selectively enforcing a security policy in a network, the method  
2    comprising the computer-implemented steps of:  
3       creating and storing one or more access controls in a policy enforcement point device  
4       that controls access of clients to the network, wherein each of the access  
5       controls specifies that a named abstract group is allowed access to a particular  
6       resource;  
7       receiving, from an external binding process, a binding of a network address to an  
8       authenticated user of one of the clients for which the policy enforcement  
9       point controls access to the network;  
10      updating the named group to include the bound network address of the authenticated  
11      user at the policy enforcement point; and  
12      permitting a packet flow originating from the network address to pass from the  
13      policy enforcement point into the network only if the network address is in  
14      the named group identified in one of the access controls that specifies that the  
15      named group is allowed access to the network.
- 1    2. A method as recited in Claim 1, wherein the steps of creating and storing one or  
2    more access controls in a policy enforcement point that controls access to the  
3    network comprise the steps of:  
4       creating and storing one or more definitions of groups in a data store;  
5       creating and storing one or more definitions of resources within a data store;  
6       creating and storing one or more access controls at the policy enforcement point,  
7       wherein each of the access controls specifies that a named group is allowed  
8       access to a particular resource, and wherein one of the access controls  
9       specifies that all other traffic is denied access to the network.
- 1    3. A method as recited in Claim 1, further comprising the steps of distributing the  
2    network address of the authenticated user and information identifying one or more  
3    groups of which the authenticated user is a member to all policy enforcement points  
4    of a protected network that the user seeks to access.

- 1       4. A method as recited in Claim 1, further comprising the steps of distributing the  
2 network address of the authenticated user and information identifying one or more  
3 groups of which the authenticated user is a member to all policy enforcement points  
4 that define a security zone that encompasses the user.
- 1       5. A method as recited in Claim 1, wherein the steps of receiving a binding of a  
2 network address to an authenticated user of a client for which the policy enforcement  
3 point controls access to the network comprises the steps of receiving an Internet  
4 Protocol (IP) address for the user from a network address binding resolution (NABR)  
5 process.
- 1       6. A method as recited in Claim 1, further comprising the steps of determining that the  
2 user has discontinued use of the client, and deleting the network address to which the  
3 user is bound from each named group of each policy enforcement point of the  
4 network.
- 1       7. A method of selectively enforcing a security policy in a network, the method  
2 comprising the computer-implemented steps of:  
3 creating and storing one or more definitions of abstract groups that are authorized to  
4 use protected resources of the network, wherein each of the definitions of  
5 abstract groups includes an abstract group name and a list of one or more  
6 network addresses of authorized users of the protected resources;  
7 creating and storing one or more access controls in a policy enforcement point device  
8 that controls access of clients to the network, wherein each of the access  
9 controls specifies that a named abstract group is allowed access to a particular  
10 resource;  
11 receiving a binding of a network address to an authenticated user of one of the clients  
12 for which the policy enforcement point controls access to the network;  
13 determining whether the bound network address of the authenticated user is in one of  
14 the lists of one of the named abstract groups; and

15 permitting a packet flow originating from the network address to pass from the  
16 policy enforcement point into the network only if the network address is in  
17 the named abstract group identified in one of the access controls that  
18 specifies that the named group is allowed access to the network.

1 8. A method as recited in Claim 7, wherein the steps of creating and storing one or  
2 more access controls in a policy enforcement point that controls access to the  
3 network comprise the steps of:

4 creating and storing one or more definitions of groups in a data store;  
5 creating and storing one or more definitions of resources within a data store;  
6 creating and storing one or more access controls at the policy enforcement point,  
7 wherein each of the access controls specifies that a named group is allowed  
8 access to a particular resource, and wherein one of the access controls  
9 specifies that all other traffic is denied access to the network.

1 9. A method as recited in Claim 7, further comprising the steps of distributing the  
2 network address of the authenticated user and information identifying one or more  
3 groups of which the authenticated user is a member to all policy enforcement points  
4 of a protected network that the user seeks to access.

1 10. A method as recited in Claim 7, further comprising the steps of distributing the  
2 network address of the authenticated user and information identifying one or more  
3 groups of which the authenticated user is a member to all policy enforcement points  
4 that define a security zone that encompasses the user.

1 11. A method as recited in Claim 7, wherein the steps of receiving a binding of a  
2 network address to an authenticated user of a client for which the policy enforcement  
3 point controls access to the network comprises the steps of receiving an Internet  
4 Protocol (IP) address for the user from a network address binding resolution (NABR)  
5 process.

TOP SECRET//  
2016  
2015  
2014  
2013  
2012  
2011  
2010  
2009  
2008

- 1    12. A method as recited in Claim 7, further comprising the steps of determining that the  
2    user has discontinued use of the client, and deleting the network address to which the  
3    user is bound from each named group of each policy enforcement point of the  
4    network.
  
- 1    13. A computer-readable medium carrying one or more sequences of instructions for  
2    selectively enforcing a security policy in a network, which instructions, when  
3    executed by one or more processors, cause the one or more processors to carry out  
4    the steps of:  
5         creating and storing one or more access controls in a policy enforcement point device  
6         that controls access of clients to the network, wherein each of the access  
7         controls specifies that a named abstract group is allowed access to a particular  
8         resource;  
9         receiving a binding of a network address to an authenticated user of one of the clients  
10      for which the policy enforcement point controls access to the network;  
11      updating the named group to include the bound network address of the authenticated  
12      user at the policy enforcement point; and  
13      permitting a packet flow originating from the network address to pass from the  
14      policy enforcement point into the network only if the network address is in  
15      the named group identified in one of the access controls that specifies that the  
16      named group is allowed access to the network.
  
- 1    14. A computer-readable medium as recited in Claim 13, wherein the instructions for  
2    carrying out the steps of creating and storing one or more access controls in a policy  
3    enforcement point that controls access to the network comprise instructions for  
4    carrying out the steps of:  
5         creating and storing one or more definitions of groups in a data store;  
6         creating and storing one or more definitions of resources within a data store;  
7         creating and storing one or more access controls at the policy enforcement point,  
8         wherein each of the access controls specifies that a named group is allowed  
9         access to a particular resource, and wherein one of the access controls  
10      specifies that all other traffic is denied access to the network.

- 1    15. A computer-readable medium as recited in Claim 13, further comprising instructions  
2        which, when executed by the one or more processors, cause the one or more  
3        processors to carry out the steps of distributing the network address of the  
4        authenticated user and information identifying one or more groups of which the  
5        authenticated user is a member to all policy enforcement points of a protected  
6        network that the user seeks to access.
- 1    16. A computer-readable medium as recited in Claim 13, further comprising instructions  
2        which, when executed by the one or more processors, cause the one or more  
3        processors to carry out the steps of distributing the network address of the  
4        authenticated user and information identifying one or more groups of which the  
5        authenticated user is a member to all policy enforcement points that define a security  
6        zone that encompasses the user.
- 1    17. A computer-readable medium as recited in Claim 13, wherein the instructions for  
2        carrying out the steps of receiving a binding of a network address to an authenticated  
3        user of a client for which the policy enforcement point controls access to the network  
4        comprise instructions for carrying out the steps of performing network address  
5        binding resolution for the user.
- 1    18. A computer-readable medium as recited in Claim 13, further comprising instructions  
2        which, when executed by the one or more processors, cause the one or more  
3        processors to carry out the steps of determining that the user has discontinued use of  
4        the client, and deleting the network address to which the user is bound from each  
5        named group of each policy enforcement point of the network.
- 1    19. An apparatus for selectively enforcing a security policy in a network, comprising:  
2        means for creating and storing one or more access controls in a policy enforcement  
3        point device that controls access of clients to the network, wherein each of the  
4        access controls specifies that a named abstract group is allowed access to a  
5        particular resource;

means for receiving a binding of a network address to an authenticated user of one of the clients for which the policy enforcement point controls access to the network;  
means for updating the named group to include the bound network address of the authenticated user at the policy enforcement point; and  
means for permitting a packet flow originating from the network address to pass from the policy enforcement point into the network only if the network address is in the named group identified in one of the access controls that specifies that the named group is allowed access to the network.

20. An apparatus for selectively enforcing a security policy in a network, comprising:  
a network interface that is coupled to the data network for receiving one or more packet flows therefrom;  
a processor;  
one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:  
creating and storing one or more access controls in a policy enforcement point device that controls access of clients to the network, wherein each of the access controls specifies that a named abstract group is allowed access to a particular resource;  
receiving a binding of a network address to an authenticated user of one of the clients for which the policy enforcement point controls access to the network;  
updating the named group to include the bound network address of the authenticated user at the policy enforcement point; and  
permitting a packet flow originating from the network address to pass from the policy enforcement point into the network only if the network address is in the named group identified in one of the access controls that specifies that the named group is allowed access to the network.
21. A method as recited in Claim 1, wherein the steps of receiving a binding of a network address to an authenticated user of a client for which the policy enforcement point controls access to the network comprises the steps of receiving an Internet Protocol (IP) address for the user from an ASAP protocol process.

- 1       22. A method as recited in Claim 1, wherein the steps of receiving a binding of a  
2       network address to an authenticated user of a client for which the policy enforcement  
3       point controls access to the network comprises the steps of receiving an Internet  
4       Protocol (IP) address for the user from a DNS process.
- 1       23. A method of selectively enforcing a security policy in a network, the method  
2       comprising the computer-implemented steps of:  
3              creating and storing one or more access control list entries in a network router that  
4              acts as a policy enforcement point device and that controls access of clients to  
5              the network, wherein each of the access control list entries specifies that a  
6              named group of users is allowed or refused access to a particular network  
7              resource;  
8              creating and storing one or more definitions of the named groups in a data store that  
9              is accessible by the network router;  
10             receiving, from an external process that can bind a user to a specific network address,  
11              a binding of a network address to an authenticated user of one of the clients  
12              for which the router controls access to the network;  
13             updating the named group to include the bound network address of the authenticated  
14              user at the policy enforcement point; and  
15             permitting a packet flow originating from the bound network address to pass from  
16              the policy enforcement point into the network only if the bound network  
17              address is in the named group identified in one of the access control list  
18              entries that specifies that the named group is allowed access to the network.
- 1       24. A method of selectively enforcing a security policy in a network, the method  
2       comprising the computer-implemented steps of:  
3              creating and storing one or more access control list entries in a network router that  
4              acts as a policy enforcement point device and that controls access of clients to  
5              the network, wherein each of the access control list entries specifies that a  
6              named group of users is allowed or refused access to a particular network  
7              resource;  
8              creating and storing one or more definitions of the named groups in a data store that  
9              is accessible by the network router;

10 receiving, from an external process that can bind a user to a specific network address,  
11 a binding of a network address to an authenticated user of one of the clients  
12 for which the router controls access to the network;  
13 updating the named group to include the bound network address of the authenticated  
14 user at the policy enforcement point;  
15 permitting a packet flow originating from the bound network address to pass from  
16 the policy enforcement point into the network only if the bound network  
17 address is in the named group identified in one of the access control list  
18 entries that specifies that the named group is allowed access to the network;  
19 and  
20 distributing the network address of the authenticated user and information identifying  
21 one or more groups of which the authenticated user is a member to all policy  
22 enforcement points that define a security zone that encompasses the user;  
23 determining that the user has discontinued use of the client, and deleting the network  
24 address to which the user is bound from each named group of each policy  
25 enforcement point of the network.